RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INDUSTRIE

SERVICE
de la PROPRIÉTÉ INDUSTRIELLE

1RE ADDITION

AU BREVET D'INVENTION

N° 1.226.403

P.V. n° 815.868 N° 76.933

Classification internationale : G 06 *b*

Générateurs perfectionnés de signaux électriques.

Société anonyme dite : SOCIÉTÉ D'ÉLECTRONIQUE ET D'AUTOMATISME résidant en France (Seine).

(*Brevet principal pris le 3 juin 1954.*)

Demandée le 15 janvier 1960, à 19 heures, par poste.

Délivrée par arrêté du 6 novembre 1961.

(*Bulletin officiel de la Propriété industrielle* n° 50 de 1961.)

(*Certificat d'addition dont la délivrance a été ajournée en exécution de l'article 11, § 7, de la loi du 5 juillet 1844 modifiée par la loi du 7 avril 1902.*)

La présente invention concerne des perfectionnements, modifications et additions apportés aux dispositions de générateurs de signaux électriques représentant des suites de nombres aléatoires, plus particulièrement destinés à la confection de tables et bandes perforées, ou similaires, d'enregistrement de ces nombres, et elle a pour but d'améliorer encore les performances de tels générateurs.

L'approche du problème de la génération d'une suite de nombres aléatoires dans le brevet principal avait conduit la demanderesse à prévoir, au brevet principal, l'établissement périodique d'un signal logique « ou exclusif » entre les conditions de deux étages de deux chaînes de comptage d'impulsions séparément alimentées par des générateurs de bruit. Toutefois, d'une part, ces étages étaient les premiers des deux chaînes de comptage et, d'autre part, et fondamentalement, les nombres d'étages de ces chaînes étaient pris importants car ladite approche concluait à la prépondérance d'un tel facteur si on désirait des lectures à intervalles rapprochés pour la génération de toute suite aléatoire d'impulsions.

Or, il est maintenant apparu à la demanderesse, dans la poursuite de ses études et réalisations, qu'un tel montage pouvait n'utiliser que des chaînes de comptage à nombre d'étages réduits pourvu que toute opération « ou exclusif » entrant en jeu soit prise entre les conditions de deux étages quelconques des chaînes de comptage car il est apparu qu'une telle opération entre deux chaînes de comptage assurait en elle-même une réduction particulièrement importante de l'erreur de la probabilité d'équirépartition des chiffres 0 et 1 dans la suite aléatoire ainsi formée.

En effet, on peut considérer des probabilités p et q dans les répartitions dans le temps de deux suites d'impulsions engendrées par des générateurs de bruit ou des chaînes de comptage d'impulsions provenant de tels générateurs de bruit, et par conséquent de deux suites de conditions d'étages en ces chaînes. La probabilité donnée par l'opération « ou exclusif » entre les nombres p et q est évidemment :

$$(1) \qquad P_{(ou)} = p.(1-q) + q.(1-p) = p - p.q + q - p.q$$
$$= p + q - 2p.q$$

Chaque probabilité peut s'exprimer, comme connu, par la relation :

$$(2) \qquad p \text{ ou } q = \frac{1}{2} + e$$

en désignant par e l'erreur d'équirépartition des 0 et 1 dans le temps, erreur qui est sensiblement uniforme pour tout générateur de bruit.

Par substitution, on a donc :

$$(3) \qquad P_{(ou)} = \frac{1}{2} + e + \frac{1}{2} + e - 2\left(\frac{1}{2} + e\right)^2 = \frac{1}{2} - 2e^2$$

Prix du fascicule : 1 NF

ce qui démontre directement une réduction importante de l'erreur.

En conformité de la présente invention, alors, on établit un dispositif générateur de signaux aléatoires en établissant deux chaînes de comptage à nombre d'étages réduit, en alimentant chaque chaîne par une suite d'impulsions de bruit et en établissant des circuits « ou exclusif » entre des étages de ces chaînes de comptage, en nombre égal au nombre de suites aléatoires de 0 et 1 désirées, ces étages étant pris arbitrairement en ces chaînes.

La figure unique jointe montre un exemple de schéma d'un tel générateur pour enregistrement de cinq pistes de ruban perforé. Ce schéma utilise deux générateurs de bruit 1 et 21 qui attaquent respectivement des formeurs d'impulsions 2 et 22 dont les sorties attaquent respectivement les entrées de deux chaînes de comptage d'impulsions 34 et 44 ayant chacune, illustrativement, cinq étages ici (elles pourraient en avoir plus ou moins si désiré). Entre les sorties de ces étages et selon un câblage arbitraire en soi, cinq opérateurs 45 à 49 assurent la formation d'autant de signaux de « ou exclusif ». Les sorties de ces opérateurs logiques aboutissent aux étages de transfert 50 dont les sorties sont dirigées sur autant d'entrées d'une perforatrice de ruban, indiquée en 51. A chaque pas de la perforatrice en sort un signal qui, modelé en 6, vient débloquer les étages 50, ce qui assure la « lecture » des conditions des circuits 45 à 49 et l'inscription des valeurs de chiffre binaire qu'elles représentent sur le ruban. Ce même signal issu de 6 pourrait, si désiré, procéder chaque fois à une remise à zéro des chaînes de comptage, ce qui n'est nullement impératif.

Au lieu d'utiliser deux générateurs de bruit matériellement distincts, on pourrait n'en utiliser qu'un, le générateur de bruit a par exemple, à condition d'insérer, entre le formeur 2 et les entrées des chaînes de comptage, un aiguilleur électronique dirigeant en alternance les impulsions de bruit sur l'une puis l'autre chaînes et ainsi de suite. Ce pourrait par exemple être un aiguillage à deux étages de transfert recevant les impulsions du formeur 2 et commandé par un multivibrateur inversant sa position environ à intervalles moitié des intervalles d'actionnement de la perforatrice.

En tous les cas, pour un code à cinq moments, le nombre d'étages de chaque chaîne ne doit pas être inférieur à trois.

On pourrait même considérer le cas où les deux chaînes de comptage seraient en série au lieu d'être en parallèle, et des circuits « ou exclusif » établis entre les deux chaînes en série (en fait les deux parties d'une chaîne d'au moins six étages alors) ; mais, comme la seconde chaîne de la série serait de fait actionnée à travers la première, donc changerait d'état moins souvent, une telle disposition s'avérerait en fait désavantageuse car il faudrait ralentir la cadence des prélèvements pour retrouver des conditions acceptables.

La technologie propre à l'exécution pratique des étages de transfert, chaînes de comptage et perforatrices n'entrent pas dans le cadre de l'invention.

RÉSUMÉ

Perfectionnement apporté aux dispositions du brevet principal, consistant principalement à établir deux chaînes de comptage, à nombre d'étages restreint, d'impulsions provenant d'au moins un générateur de bruit et appliquées en deux suites sur ces deux chaînes, et à établir un ou plusieurs circuits « ou exclusif » entre des étages, pris au hasard, de l'une et l'autre de ces chaînes.

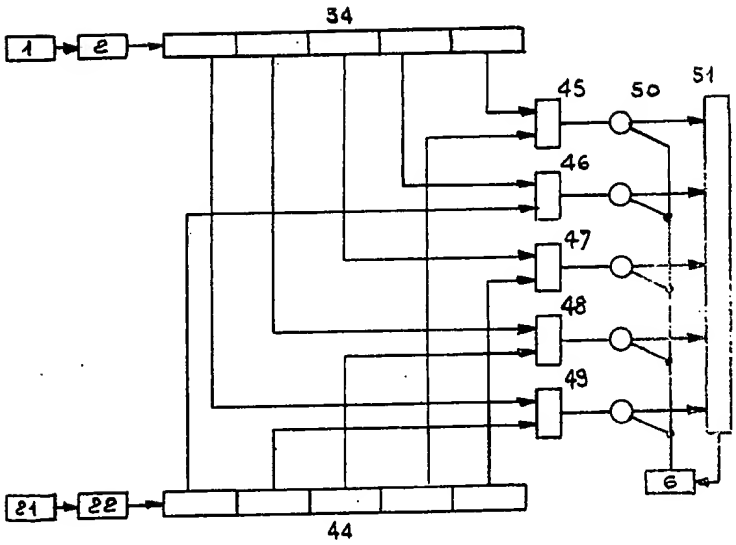
Produits industriels nouveaux constitués par les générateurs de signaux aléatoires incorporant ces nouvelles dispositions, en toutes variantes de mise en pratique et d'exploitation.

Société anonyme dite :
SOCIÉTÉ D'ÉLECTRONIQUE ET D'AUTOMATISME
Par procuration :
H.-D. TASSY

Pour la vente des fascicules, s'adresser à l'IMPRIMERIE NATIONALE, 27, rue de la Convention, Paris (15e).

N. 76.933 Société Anonyme dite : Pl. unique

Société d'Électronique et d'Automatisme



RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INDUSTRIE

SERVICE
de la PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION

P.V. n° 670.304 N° 1.226.403

Classification internationale G 06 *k*

Générateurs perfectionnés de signaux électriques. (Invention : Jean-Henri LEMOINE et Claude-Olivier LEPAGE.)

Société anonyme dite : SOCIÉTÉ D'ÉLECTRONIQUE ET D'AUTOMATISME résidant en France (Seine).

Demandé le 3 juin 1954, à 10h 25m, à Paris.
Délivré le 29 février 1960. — Publié le 11 juillet 1960.
(*Brevet d'invention dont la délivrance a été ajournée en exécution de l'article 11, § 7, de la loi du 5 juillet 1844 modifiée par la loi du 7 avril 1902.*)

La présente invention concerne des générateurs de signaux électriques représentant des suites de nombres aléatoires, du genre de ceux dans lesquels une source de signaux aléatoires (mouvement brownien, agitation thermique d'une cathode, etc.) envoie des impulsions à un compteur par l'intermédiaire d'un organe à seuil d'amplitude, ce par quoi ledit compteur est actionné comme s'il recevait une suite d'impulsions à cadence irrégulière et ce par quoi alors, en effectuant la lecture périodique dudit compteur, en son ou ses étages de plus faibles poids numériques, on obtient à chaque lecture un nombre aléatoire à un ou plusieurs chiffres. Par le groupement de ces nombres, seuls ou en juxtaposition avec d'autres similairement obtenus, on peut alors réaliser une suite de nombres aléatoires. Une telle suite, ou tel ensemble de nombres aléatoires, sera ici dénommé « table ».

Pour qu'une telle table puisse être avantageusement utilisée en tous systèmes codés et chiffrés, il convient que les nombres qui la composent soient également équirépartis, ou à tout le moins présentent une bonne approximation de cette équipartition; la suite des nombres alors contenus dans la table représentant une fonction aléatoire stationnaire à accroissement indépendant.

Cette condition ne peut être approximativement satisfaite toutefois, avec un générateur du genre sus-spécifié, qu'au prix d'une certaine lenteur d'opération, résultant de la nécessité de n'effectuer les lectures du compteur qu'à des intervalles de temps relativement larges.

En effet, en admettant que la probabilité d'avoir au moins un événement (ici une impulsion) dans un intervalle de temps de largeur définie, soit t, ne dépend que de la largeur de cet intervalle, la probabilité d'obtenir un nombre n d'événements dans cet intervalle de temps est donnée par la loi de Poisson :

$$(1) \qquad P = e^{-kt} \cdot \frac{(kt)^n}{n},$$

relation dans laquelle le facteur désigné par k est le nombre statistique moyen d'événements dans l'unité de temps, eu égard à la source de signaux aléatoires considérée. Pour des raisons évidentes d'ordre technologique, ce facteur k est quasi imposé par cette source.

En considérant, pour simplifier ici l'exposé, que les impulsions sont comptées dans un compteur binaire, leur totalisation s'effectuant donc dans le système de numération de base 2, la probabilité pour que le dernier chiffre inscrit dans l'étage de plus petit poids binaire du compteur soit 0, donc que le nombre compté soit pair, est donnée par la série :

$$(2) \qquad P_0 = e^{-kt} \cdot \left(1 + \frac{(kt)^2}{2} + \frac{(kt)^4}{4} + \frac{(kt)^6}{6} + \ldots\right)$$

d'où

$$(3) \qquad P_0 = \frac{1}{2}\left(1 + e^{-2kt}\right),$$

alors que la probabilité pour que le nombre soit impair et se termine par 1, est :

$$(4) \qquad P_1 = \frac{1}{2}\left(1 - e^{-2kt}\right).$$

Pour réduire au mieux l'inégalité entre les deux valeurs des facteurs P_0 et P_1, jusqu'à présent, on a simplement prévu de façon directe de prendre la valeur de l'intervalle de temps moyen entre deux lectures consécutives du compteur très grande, afin de rendre très petit, en conséquence, le facteur e^{-2kt}.

Pour souligner l'inconvénient de l'inégalité des deux expressions P_0 et P_1 au point de vue du manque d'équirépartition des nombres aléatoires

Prix du fascicule : 1 NF

obtenus, et pour donner indicativement par ailleurs, un exemple de mode de formation de tables de nombres aléatoires, on peut considérer que, dans cette table, les chiffres qui ont respectivement même poids dans les colonnes de la table ont été obtenus par la lecture à intervalles de largeur t, de la condition du premier étage (0 ou 1) d'un compteur binaire inclus dans un système du genre spécifié. Alors, et en supposant que ce compteur a été remis à zéro après chaque lecture de son premier étage, la série des nombres contenus dans cette table contiendra :

Plus de nombres pairs que de nombres impairs;

Plus de nombres divisibles par 4 que de nombres pairs non divisibles par 4;

Plus de nombres divisibles par 8 que de nombres divisibles par 4 et non par 8, etc.

Si le compteur n'avait pas été remis à zéro après chaque lecture, la série de nombres contenus dans ladite table obéirait à un processus de Markoff.

Des démonstrations similaires pourraient être faites pour d'autres bases de numération que la binaire. Elles conduiraient à des conclusions similaires et, en pratique, à considérer qu'il faut *a priori* prendre très grande la valeur t de tout intervalle de temps entre lectures du compteur en toute disposition usuelle de générateur de nombres aléatoires.

L'invention se propose de perfectionner les générateurs de nombres aléatoires du genre susdit de manière à permettre au contraire à accélérer la formation des chiffres de ces nombres par réduction substantielle des intervalles de temps entre lectures du compteur incorporé à l'appareil, et ce, dans des conditions d'équiprobabilité des nombres finalement obtenus au moins aussi satisfaisantes qu'avec les appareils à fonctionnement systématiquement ralenti de la technique antérieure.

Et elle vise, surtout à titre de produits industriels nouveaux, les générateurs de nombres aléatoires ainsi accélérés en leur fonctionnement propre, aussi bien pour l'établissement de tables par impression des nombres débités que, par voie de conséquence de cette accélération d'opération, pour l'établissement de générateurs de signaux de clés de chiffrement dans les systèmes de chiffrement direct de signaux clairs.

L'invention se caractérise à ces fins et de façon générale par la prévision, dans un générateur de signaux aléatoires qui comporte au moins une source de signaux aléatoires, un compteur d'impulsions actionné par ladite source à travers un organe à seuil d'amplitude et des moyens propres à effectuer à intervalles la lecture de la condition d'au moins le premier étage de ce compteur, assurer sa remise à zéro à chaque lecture, et transmettre les signaux résultant de ces lectures à au moins une voie de prélèvement, de moyens propres à engendrer une suite auxiliaire d'impulsions au moins et à commander par cette suite d'impulsions une modification de la séquence des signaux prélevés du compteur principal telle que soient sensiblement égalisées les probabilités des facteurs dominants de ces signaux en cette séquence, ce par quoi la durée propre aux intervalles de lecture devient sans importance au point de vue de l'équirépartition des nombres aléatoires formés et peut, par suite, être prise très courte sans que soit altéré le bon fonctionnement de l'ensemble à ce dernier point de vue.

Elle se caractérise plus particulièrement en prévoyant d'engendrer une telle suite auxiliaire d'impulsions par ou sous la commande d'un compteur additionnel, et plus particulièrement alors, en prévoyant pour ce compteur additionnel, sa commande et l'exploitation des impulsions engendrées ou contrôlées par lui, les principales dispositions suivantes, séparément ou en toute combinaison techniquement valable :

a. Le compteur auxiliaire est actionné par certains des signaux résultant de la lecture du compteur principal;

b. Le compteur auxiliaire est actionné par les impulsions servant aussi à la lecture du compteur principal;

c. Le compteur auxiliaire est actionné par des impulsions provenant d'une source aléatoire additionnelle;

d. Les impulsions auxiliaires sont délivrées par le dernier étage dudit compteur auxiliaire;

e. Les impulsions auxiliaires sont formées par sélection des impulsions de lecture sous la commande de la condition de ce compteur auxiliaire;

f. Les impulsions auxiliaires résultent d'une lecture répétée de la condition d'un étage au moins de ce compteur auxiliaire;

g. Les impulsions auxiliaires sont combinées avec certains des signaux formés par lecture du compteur principal;

h. Les impulsions auxiliaires sont combinées avec la totalité de ces signaux;

i. La combinaison selon *g* consiste en une inhibition des signaux provenant du compteur principal;

j. La combinaison selon *g* consiste en une addition sans retenue des impulsions auxiliaires aux signaux du compteur principal;

k. Les impulsions auxiliaires sont combinées avec les impulsions d'actionnement du compteur principal;

l. La combinaison selon *k* consiste en une inhibition de ces impulsions en leur action sur le compteur principal;

m. La combinaison selon *k* consiste en une totalisation des impulsions auxiliaires aux impulsions d'actionnement du compteur principal.

Ces dispositions, ainsi que d'autres encore, et

leurs modalités de mise en œuvre et d'exploitation pratique, vont être exposées dans le détail en se reportant à un cas illustrativement considéré, celui de la formation de suites de signaux aléatoires par un compteur binaire, dont le premier étage est seul soumis à une lecture répétée (périodique ou non) à brefs intervalles de temps. En ce cas, divers exemples de réalisation sont schématiquement représentés sur les fig. 1 à 5, jointes, qui montrent chacune, à titre non limitatif, une organisation de générateur de signaux aléatoires conforme à la présente invention :

La fig. 1 est un schéma où le compteur auxiliaire est actionné par les impulsions prélevées sur la voie de lecture du compteur principal pour la condition 0 de son premier étage;

La fig. 2 est un schéma où le compteur auxiliaire est actionné en permanence par le générateur d'impulsions de lecture du compteur principal et les impulsions auxiliaires sont totalisées dans le compteur principal avec ses impulsions d'actionnement propres;

La fig. 3 est une variante de la fig. 2 où le compteur auxiliaire est actionné à partir d'un générateur aléatoire auxiliaire;

La fig. 4 est une variante de la fig. 3, en laquelle les impulsions auxiliaires sont combinées avec les signaux lus sur le compteur principal;

La fig. 5 est un schéma symétrisé de la variante de la fig. 4, le compteur auxiliaire ayant même configuration que le compteur principal et étant lui-même lu à la même cadence que ce dernier.

Dans ces figures, la référence numérique 1 désigne une source de bruits de toute nature désirée et la référence 2 désigne un organe à seuil d'amplitude ne transmettant que les crêtes d'amplitude, d'une ou des deux polarités du signal fluctuant délivré par la source, cet organe pouvant avantageusement incorporer aussi un modeleur assurant une présentation de ces crêtes avec une forme correcte pour l'actionnement d'un compteur d'impulsions. Ce dernier est désigné par la référence numérique 4 et c'est de son premier étage 3 que seront tirés les signaux aléatoires. A cette fin, les plaques des deux tubes de cet étage 3, étage basculeur conventionnel de tout compteur binaire d'ailleurs, sont par exemple reliées aux électrodes de commande de conductibilité de deux tubes 8 et 9, en sorte que, selon la condition de l'étage 3 l'un de ces tubes soit passant et l'autre non-passant et vice versa pour la condition inverse de l'étage basculeur. En place de tubes, on pourrait utiliser des réseaux d'éléments unidirectionnels bien entendu. Un générateur d'impulsions 6, rythmé ou non, applique ses impulsions sur les deux tubes 8 et 9 et par suite seule sera transmise sur la voie de prélèvement correspondante, 10 ou 11, l'impulsion qui trouve le tube 8 ou le tube 9, respectivement, passant. Pour la commodité de l'exposé, on considérera que le tube 8 est passant lorsque l'étage 3 est au repos (chiffre pair), et affiche donc la valeur 0; toute impulsion délivrée par le tube 8 représentera donc un zéro. Similairement, toute impulsion délivrée par le tube 9 représentera le chiffre un (nombre impair). Les voies de prélèvement 10 et 11 pourront être ultérieurement réunies, l'une d'elles comportant auparavant un inverseur de polarité par exemple pour discriminer finalement les deux valeurs de chiffre 0 et 1

Chaque impulsion délivrée par le générateur 6 est, après un léger retard en 7, appliquée comme impulsion de remise à zéro des étages du compteur 4, sinon le fonctionnement suivrait un processus de Markoff, comme dit.

Cet ensemble d'éléments constitue un générateur usuel de signaux aléatoires et par suite, les probabilités de délivrance des 0 et des 1 sont telles qu'indiquées en début d'exposé, relations 3 et 4. Il s'agit d'égaliser au mieux les valeurs de ces probabilités sans devoir, pour cela, prendre très petit le facteur e^{-kt}, donc l'intervalle t entre lectures grand.

Dans le schéma de la fig. 1, un compteur auxiliaire 13 est prévu pour compter les impulsions sortant du tube 8, donc celles qui représentent des. 0. La sortie d'impulsion du dernier étage du compteur 13 commande la conductibilité d'un étage de transfert 14 inséré dans la voie de prélèvement 10, pour que, chaque fois que cet étage délivre une impulsion de retour au repos après actionnement (lors donc que le compteur revient à zéro), l'étage 14 soit rendu non-passant et bloque l'impulsion figurative d'un 0 qui a provoqué ce retour. Un élément de retard 12 est introduit dans la voie de prélèvement entre le tube 8 et l'étage 14 pour ajuster la coïncidence entre impulsions de 0 et impulsions d'inhibition sur l'étage 14. Par ce moyen, et en désignant par n le nombre d'étages du compteur auxiliaire 13, on commande la transmission des impulsions représentant les 0 par une suite auxiliaire formée sous le contrôle de ces impulsions mêmes. Toute $(n+1)^e$ impulsion de 0 sera supprimée dans le prélèvement.

En prévoyant alors le nombre n, entier, tel que l'on ait :

$$1 - e^{-2kt} = n/(n+1) \tag{5}$$

sensiblement, on aura introduit un accident à la probabilité des 0 qui compensera ainsi en pratique l'inégalité des probabilités P_0 et P_1 telles que susindiquées.

On pourrait en variante assurer cet accident en prenant le compteur 13 à $2n$ étages et en dirigeant sa sortie directement sur la voie 11 (étage 14 maintenu); ceci éviterait l'absence de toute indi-

cation à un instant de lecture, ce qui est le cas pour la disposition précédente.

Dans le schéma de la fig. 2, le compteur auxiliaire 15, est alimenté directement par les impulsions de lecture provenant du générateur 6, la condition de son dernier étage, statique, commande la condition de conductibilité d'un étage de transfert 16 dont l'autre entrée reçoit ces mêmes impulsions de lecture. Ainsi, si la capacité du compteur 15 est N, pendant N/2 impulsions l'étage de transfert 16 sera passant et il sera non-passant pendant les N/2 impulsions suivantes. Il est bien évident que ces conditions de conductibilité de l'étage 16 alterneront puisque le fonctionnement du compteur 15 est périodique.

Un demi- additionneur 17 (délivrant une impulsion s'il en reçoit une seule, ne délivrant pas d'impulsions s'il en reçoit deux concomitamment ou quasi concomitamment), est intercalé entre le formeur d'impulsions 2 provenant de la source aléatoire 1 et l'entrée d'actionnement du compteur principal 4. L'autre entrée de ce demi-additionneur 17 est reliée à la sortie de l'étage de transfert 16.

Par suite, pendant N/2 lectures, en alternance, une impulsion additionnelle sera ajoutée au contenu du compteur principal tel que fourni par les signaux de la source aléatoire 1 ou ne sera pas ajoutée à ce contenu. L'application des impulsions de lecture sur les tubes 8 et 9 est légèrement retardée comme indiqué en 34 pour que la lecture s'effectue après l'addition en 17.

De ce fait, résulte une inversion périodique des probabilités P_0 et P_1 puisqu'en fait, la disposition de la fig. 2 consiste à assurer une inversion périodique des voies de prélèvement 10 et 11. Il est par suite bien évident qu'en une variante, non figurée, la sortie du compteur 15, compteur binaire bien entendu, pourrait commander un montage inversant les sorties des tubes 8 et 9 sur les voies de prélèvement 10 et 11 au rythme N/2 susdit.

Afin d'éviter cependant l'introduction d'un élément de périodicité dans la formation des nombres aléatoires qui, bien que difficilement décelable, existe de façon évidente, on peut alors substituer à l'actionnement du compteur 15 par le générateur d'impulsions 6, fig. 2, l'actionnement d'un compteur, d'ailleurs similaire 20 par le moyen d'une source aléatoire auxiliaire 18 alimentant ledit compteur 20 par l'intermédiaire de l'organe à seuil et modeleur 19. La périodicité susdite est ainsi rompue. Comme le compteur 20 a une capacité réduite vis-à-vis de celle du compteur principal et que d'autre part l'organe 19 peut être établi pour travailler à un seuil différent de celui de l'organe 2, on peut, en une variante alors évidente, omettre la source 18 et alimenter l'organe 19 par les signaux de la source 1.

Au lieu de totaliser les impulsions provenant de l'étage 16 dans le compteur principal on peut, tout aussi bien et avec le même résultat pratique d'égalisation des probabilités des 0 et des 1, totaliser ces impulsions (seulement délivrées lorsque l'étage 16 est passant, donc pour une moitié seulement de la capacité du compteur 20, en alternance aux temps de fermeture de cet étage 16 pour l'autre moitié de la capacité du compteur), aux impulsions provenant aussi bien de la lecture de l'étage 8 que de l'étage 9 du compteur principal. Cette disposition est représentée sur la fig. 4 où la sortie de l'étage 16 est reliée à une entrée d'un demi-additionneur 30, recevant sur son autre entrée les impulsions représentant les 0, et aussi à une entrée d'un demi-additionneur 31, recevant sur son autre entrée les impulsions représentant les 1. Ces demi-additionneurs sont sans reports de retenue. Comme les impulsions des 0 et des 1 ne sont évidemment pas concomitantes dans les lectures, les voies de prélèvement sont par suite inversées de fait à la cadence variable fournie par le compteur 20.

Enfin, il est également possible, fig. 5, de disposer de deux ensembles de même constitution mais alimentés par des sources de bruit indépendantes 1 et 21. Les impulsions formées en 2 et 22 sont dirigées indépendamment vers les entrées des compteurs respectifs 4 et 24. Les lectures des conditions des premiers étages 3 et 23 de ces compteurs sont assurées par le même générateur 6 qui, après retard en 7 et 27 de ses impulsions propres, remet aussi à zéro les deux compteurs. Les tubes 8 et 28 délivreront respectivement les impulsions représentant les chiffres 1, les tubes 9 et 29, les impulsions représentant les chiffres 0. On dispose deux additionneurs ou demi-additionneurs sans reports de retenues 32 et 33. L'un reçoit sur ses entrées les signaux de sortie des tubes 8 et 29, l'autre similairement les signaux de sortie des tubes 9 et 28. Comme les conditions respectives des premiers étages 3 et 23 sont bien évidemment arbitraires vis-à-vis l'une de l'autre à tous instants de lecture, le groupement prévu assure une probabilité sur chaque voie de prélèvement qui peut s'exprimer par :

$$P = \frac{1}{2}(1 + e^{-4kt}). \qquad (6)$$

Cette dernière disposition toutefois nécessite un équipement non négligeable et n'apporte en fait qu'un gain de deux en vitesse d'opération, ceci de façon évidente en soi.

D'autres variations dans les schémas donnés apparaîtront clairement de ce qui précède sans qu'il soit besoin d'en poursuivre la description détaillée.

Par ailleurs, l'adaptation des dispositions susdites à des générateurs de nombres aléatoires à plusieurs chiffres, binaires ou décimaux, est directe

et n'a par suite pas besoin non plus d'être considérée plus avant.

RÉSUMÉ

Générateurs de signaux électriques représentant des nombres aléatoires, pour la formation de suites de tels nombres à exploiter en chiffrements directs ou non de signaux, du genre de ceux dans lesquels les signaux figuratifs des chiffres de ces nombres sont obtenus par lectures répétées de la condition d'un étage au moins de plus petit poids d'un compteur d'impulsions actionné par des impulsions formées à partir de la tension de sortie d'une source de bruits, et perfectionnés en ce qu'afin d'égaliser les probabilités d'occurrence en ces lectures des différentes valeurs de chiffre à considérer, plus particulièrement dans le but de permettre une cadence élevée des lectures répétées de ce compteur, des moyens sont aussi prévus et incorporés à ces générateurs pour former au moins une suite d'impulsions auxiliaires et commander par cette suite d'impulsions une modification telle de la séquence des signaux aléatoires engendrés que soit égalisées au mieux les probabilités susdites; lesdites impulsions auxiliaires étant engendrées par un compteur auxiliaire au moins, actionné soit par des impulsions mêmes de chiffre telles que lues soit par des impulsions servant par ailleurs auxdites lectures, soit encore par des impulsions dérivées d'une source aléatoire de bruits; lesdites impulsions auxiliaires étant d'autre part soit directement dérivées de la sortie de ce compteur, soit dérivées par lecture d'un étage au moins de ce compteur et alors, de préférence, par les impulsions mêmes de lecture du compteur principal; et ces dites impulsions auxiliaires étant, selon les besoins, appliquées à la commande de permutations, périodiques ou non, entre les voies de prélèvement des impulsions résultant de la lecture du compteur principal, que cette permutation s'effectue directement sur ces voies, par inhibition et (ou) transfert, ou additions sans retenues des impulsions résultant de la lecture auxdites impulsions auxiliaires, soit indirectement par totalisation desdites impulsions auxiliaires dans ledit compteur principal avec ses impulsions d'actionnement propres.

Produits industriels nouveaux constitués par des générateurs incorporant, pour partie au moins, les dispositions ci-dessus, en toutes variantes d'exécution, ainsi que par les ensembles de chiffrement ou déchiffrement qui les incorporent en tant que générateurs de signaux de clés ou par les appareils à établir des tables de chiffrement qui les incorporent en tant que générateurs de signaux aléatoires à imprimer ou enregistrer.

Société anonyme dite :
SOCIÉTÉ D'ÉLECTRONIQUE ET D'AUTOMATISME
Par procuration :
H.-D. TASSY

Pour la vente des fascicules, s'adresser à l'IMPRIMERIE NATIONALE, 27, rue de la Convention, Paris (15e).

Société d'Électronique et d'Automobiles

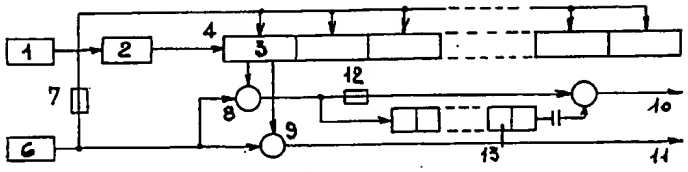


FIG.1

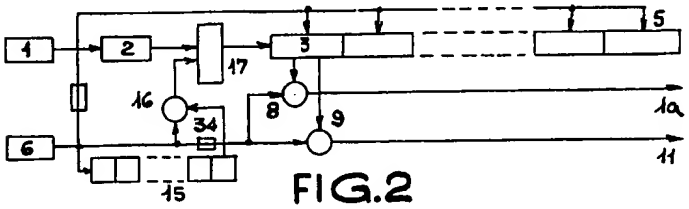


FIG.2

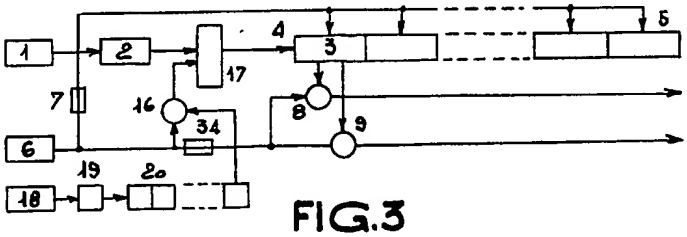


FIG.3

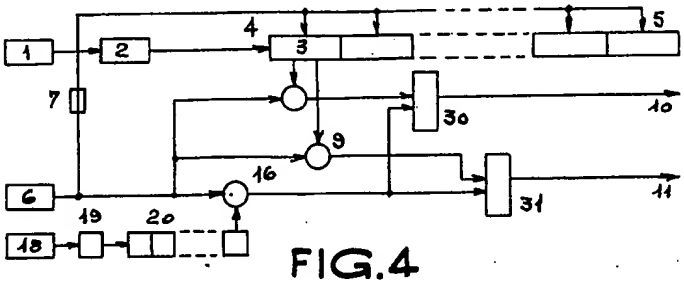


FIG.4

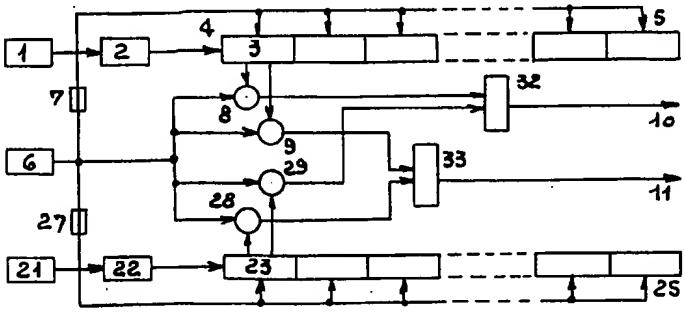


FIG.5